2005 DRAFTING REQUEST

Senate Substitute Amendment (SSA-SB164)

Received: **09/13/2005**

Received By: **csundber**

Wanted: **As time permits**

Identical to LRB:

For: **Ted Kanavas (608) 266-9174**

By/Representing: **Mike Richards**

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - other**

Extra Copies:

Submit via email: **YES**

Requester's email: **Sen.Kanavas@legis.state.wi.us**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Delete email addresses, 30-day deadline, modify exemption for regulated entities

---

Instructions:

See Attached

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	csundber 09/14/2005	lkunkel 09/15/2005		_____ _____			
/1			pgreensl 09/15/2005	_____ _____	lemery 09/15/2005	lemery 09/15/2005	

FE Sent For:

<END>

2005 DRAFTING REQUEST

Senate Substitute Amendment (SSA-SB164)

Received: **09/13/2005**

Received By: **csundber**

Wanted: **As time permits**

Identical to LRB:

For: **Ted Kanavas (608) 266-9174**

By/Representing: **Mike Richards**

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - other**

Extra Copies:

Submit via email: **YES**

Requester's email: **Sen.Kanavas@legis.state.wi.us**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Delete email addresses, 30-day deadline, modify exemption for regulated entities ✓

Instructions:

See Attached

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	csundber	1/1 lmk 9/14	9/15 pg	9/15 9/19			

FE Sent For:

<END>

9/13 Mike Richards (Kanavas)

Changes to Sub to SB 164

1. P.2 l. 15: remove email addresses
2. P.4 l. 10: remove 30-day deadline
3. Regulated entities: MR will call back re add'l language dealing with entities subject to ~~HIPAA~~.

nationwide consumer reporting agencies. The commenter stated that the nationwide consumer reporting agencies spent approximately $1.5 million per company, handling approximately 365,000 inquiries from the company's customers.

The final Guidance contains a number of changes that will diminish the costs identified by these commenters. First, the standard for notification in the final Guidance likely will result in fewer notices. In addition, the final Guidance no longer states that all notices should advise customers to contact the nationwide consumer reporting agencies. Therefore, the Agencies' estimates do not factor in the costs to the reporting agencies.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act applies only to rules for which an agency publishes a general notice of proposed rulemaking pursuant to 5 U.S.C. 553(b). *See* 5 U.S.C. 601(2). As previously noted, a general notice of proposed rulemaking was not published because this final Guidance is a general statement of policy. Thus, the Regulatory Flexibility Act does not apply to the final Guidance.

With respect to OTS's revision to its regulation at 12 CFR 568.5, as noted above, OTS has concluded that there is good cause to dispense with prior notice and comment. Accordingly, OTS has further concluded that the Regulatory Flexibility Act does not apply to this final rule.

C. Executive Order 12866

The OCC and OTS have determined that this final Guidance is not a significant regulatory action under Executive Order 12866. With respect to OTS's revision to its regulation at 12 CFR 568.5, OTS has further determined that this final rule is not a significant regulatory action under Executive Order 12866.

D. Unfunded Mandates Reform Act of 1995

The OCC and OTS have determined that this final Guidance is not a regulatory action that would require an assessment under the Unfunded Mandates Reform Act of 1995 (UMRA), 2 U.S.C. 1531. The final Guidance is a general statement of policy and, therefore, the OCC and OTS have determined that the UMRA does not apply.

With respect to OTS's revision to its regulation at 12 CFR 568.5, as noted above, OTS has concluded that there is good cause to dispense with prior notice and comment. Accordingly, OTS has concluded that the UMRA does not require an unfunded mandates analysis.

Text of Common Final Guidance

The text of the Agencies' common final Guidance reads as follows:

Supplement A to Appendix _ to Part _—Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

I. Background

This Guidance [1] interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines")[2] and describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The scope of, and definitions of terms used in, this Guidance are identical to those of the Security Guidelines. For example, the term "customer information" is the same term used in the Security Guidelines, and means any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution.

A. Interagency Security Guidelines

Section 501(b) of the GLBA required the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction that include administrative, technical, and physical safeguards, to protect the security and confidentiality of customer information. Accordingly, the Agencies issued Security Guidelines requiring every financial institution to have an information security program designed to:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

B. Risk Assessment and Controls

1. The Security Guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and

c. The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.[3]

2. Following the assessment of these risks, the Security Guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines,[4] and adopt those that are appropriate for the institution, including:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Background checks for employees with responsibilities for access to customer information; and

c. Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[5]

C. Service Providers

The Security Guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[6]

II. Response Program

Millions of Americans, throughout the country, have been victims of identity theft.[7] Identity thieves misuse personal information they obtain from a number of sources, including financial institutions, to perpetrate identity theft. Therefore, financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial

[1] This Guidance is being jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

[2] 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D–2 and part 225, app. F (Board); 12 CFR part 364, app. B (FDIC); and 12 CFR part 570, app. B (OTS). The "Interagency Guidelines Establishing Information Security Standards" were formerly known as "The Interagency Guidelines Establishing Standards for Safeguarding Customer Information."

[3] *See* Security Guidelines, III.B.

[4] *See* Security Guidelines, III.C.

[5] *See* Security Guidelines, III.C.

[6] *See* Security Guidelines, II.B. and III.D. Further, the Agencies note that, in addition to contractual obligations to a financial institution, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission ("FTC"), 12 CFR part 314.

[7] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identity theft in 2002. *See* The Federal Trade Commission, *Identity Theft Survey Report*, (September 2003), available at *http://www.ftc.gov/os/2003/09/synovatereport.pdf.*

institutions should place access controls on customer information systems and conduct background checks for employees who are authorized to access customer information.[8] However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems[9] that occur nonetheless. A response program should be a key part of an institution's information security program.[10] The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to customer information in customer information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in the Guidelines that relate to these arrangements, and with existing guidance on this topic issued by the Agencies,[11] an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

A. Components of a Response Program

1. At a minimum, an institution's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below;

c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations,[12] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;[13] and

e. Notifying customers when warranted.

2. Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's customers or regulator on its behalf.

III. Customer Notice

Financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. Notifying customers of a security incident involving the unauthorized access or use of the customer's information in accordance with the standard set forth below is a key part of that duty. Timely notification of customers is important to manage an institution's reputation risk. Effective notice also may reduce an institution's legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft. When customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

1. Sensitive Customer Information

Under the Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is most likely to be misused, as in the commission of identity theft. For purposes of this Guidance, *sensitive customer information* means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. *Sensitive customer information* also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

2. Affected Customers

If a financial institution, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the institution determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

B. Content of Customer Notice

1. Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the

[8] Institutions should also conduct background checks of employees to ensure that the institution does not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).

[9] Under the Guidelines, an institution's *customer information systems* consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. *See* Security Guidelines, I.C.2.d (I.C.2.c for OTS).

[10] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002 available at *http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm.* Federal Reserve SR 97–32, Sound Practice Guidance for Information Security for Networks, Dec. 4, 1997; OCC Bulletin 2000–14, "Infrastructure Threats—Intrusion Risks" (May 15, 2000), for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[11] *See* Federal Reserve SR Ltr. 00–04, Outsourcing of Information and Transaction Processing, Feb. 9, 2000; OCC Bulletin 2001–47, "Third-Party Relationships Risk Management Principles," Nov. 1, 2001; FDIC FIL 68–99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999; OTS Thrift Bulletin 82a, Third Party Arrangements, Sept. 1, 2004.

[12] An institution's obligation to file a SAR is set out in the Agencies' SAR regulations and Agency guidance. *See* 12 CFR 21.11 (national banks, Federal branches and agencies); 12 CFR 208.62 (State member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured State branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (State non-member banks); and 12 CFR 563.180 (savings associations). National banks must file SARs in connection with computer intrusions and other computer crimes. *See* OCC Bulletin 2000–14, "Infrastructure Threats—Intrusion Risks" (May 15, 2000); Advisory Letter 97–9, "Reporting Computer Related Crimes" (November 19, 1997) (general guidance still applicable though instructions for new SAR form published in 65 FR 1229, 1230 (January 7, 2000)). *See also* Federal Reserve SR 01–11, Identity Theft and Pretext Calling, Apr. 26, 2001; SR 97–28, Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions, Nov. 6, 1997; FDIC FIL 48–2000, Suspicious Activity Reports, July 14, 2000; FIL 47–97, Preparation of Suspicious Activity Reports, May 6, 1997; OTS CEO Memorandum 139, Identity Theft and Pretext Calling, May 4, 2001; CEO Memorandum 126, New Suspicious Activity Report Form, July 5, 2000; *http://www.ots.treas.gov/BSA* (for the latest SAR form and filing instructions required by OTS as of July 1, 2003).

[13] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002, pp. 68–74.

customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance.[14] The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution. The notice should include the following additional items, when appropriate:

a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;

b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;

c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the customer may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.[15]

2. The Agencies encourage financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

C. Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Adoption of Final Guidance

The agency-specific adoption of the common final Guidance, which appears at the end of the common preamble, follows.

[14] The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

[15] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.consumer.gov/idtheft* and 1–877–IDTHEFT. The institution may also refer customers to any materials developed pursuant to section 151(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).

List of Subjects

12 CFR Part 30

Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 208

Banks, banking, Consumer protection, Information, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 225

Banks, banking, Holding companies, Reporting and recordkeeping requirements.

12 CFR Part 364

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

12 CFR Part 568

Consumer protection, Privacy, Reporting and recordkeeping requirements, Savings associations, Security measures.

12 CFR Part 570

Accounting, Administrative practice and procedure, Bank deposit insurance, Consumer protection, Holding companies, Privacy, Reporting and recordkeeping requirements, Safety and soundness, Savings associations.

Department of the Treasury

Office of the Comptroller of the Currency

12 CFR CHAPTER I

Authority and Issuance

■ For the reasons set out in the joint preamble, the OCC amends part 30 of chapter I of title 12 of the Code of Federal Regulations to read as follows:

PART 30—SAFETY AND SOUNDNESS STANDARDS

■ 1. The authority citation for part 30 continues to read as follows:

Authority: 12 U.S.C. 93a, 371, 1818, 1831p, 3102(b); 15 U.S.C. 1681s, 1681w, 6801, 6805(b)(1).

■ 2. Revise the heading of Appendix B to read as follows:

Appendix B to Part 30—Interagency Guidelines Establishing Information Security Standards

* * * * *

■ 3. Amend Appendix B to part 30 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

Dated: March 8, 2005.

Julie L. Williams,

Acting Comptroller of the Currency.

FEDERAL RESERVE SYSTEM

12 CFR CHAPTER II

Authority and Issuance

■ For the reasons set out in the joint preamble, the Board amends part 208 and 225 of chapter II of title 12 of the Code of Federal Regulations to read as follows:

PART 208—MEMBERSHIP OF STATE BANKING INSTITUTIONS IN THE FEDERAL RESERVE SYSTEM (REGULATION H)

■ 1. The authority citation for 12 CFR part 208 continues to read as follows:

Authority: 12 U.S.C. 24, 36, 92a, 93a, 248(a), 248(c), 321–338a, 371d, 461, 481–486, 601, 611, 1814, 1816, 1820(d)(9), 1823(j), 1828(o), 1831, 1831o, 1831p–1, 1831r–1, 1831w, 1831x, 1835a, 1882, 2901–2907, 3105, 3310, 3331–3351, and 3906–3909, 15 U.S.C. 78b, 78l(b), 78l(g), 78l(i), 78o–4(c)(5), 78q, 78q–1, 78w, 1681s, 1681w, 6801 and 6805; 31 U.S.C. 5318, 42 U.S.C. 4012a, 4104a, 4104b, 4106, and 4128.

■ 2. Revise the heading of Appendix D–Z to read as follows:

Appendix D–2 to Part 208—Interagency Guidelines Establishing Information Security Standards.

* * * * *

■ 3. Amend Appendix D–2 to part 208 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

PART 225—BANK HOLDING COMPANIES AND CHANGE IN BANK CONTROL (REGULATION Y)

■ 4. The authority citation for 12 CFR part 225 is revised to read as follows:

Authority: 12 U.S.C. 1817(j)(13), 1818, 1828(o), 1831i, 1831p–1, 1843(c)(8), 1844(b), 1972(1), 3106, 3108, 3310, 3331–3351, 3906, 3907, and 3909; 15 U.S.C. 1681s, 1681w, 6801 and 6805.

■ 5. Revise the heading of Appendix F to read as follows:

Appendix F to Part 225—Interagency Guidelines Establishing Information Security Standards

* * * * *

■ 6. Amend Appendix F to part 225 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

By order of the Board of Governors of the Federal Reserve System, March 21, 2005.

Jennifer J. Johnson,

Secretary of the Board.

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR CHAPTER III

Authority and Issuance

■ For the reasons set out in the joint preamble, the FDIC amends part 364 of chapter III of title 12 of the Code of Federal Regulations to read as follows:

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

■ 1. The authority citation for part 364 is revised to read as follows:

Authority: 12 U.S.C. 1818 and 1819 (Tenth); 15 U.S.C. 1681b, 1681s, and 1681w.

■ 2. Revise the heading of Appendix B to read as follows:

Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards

* * * * *

■ 3. Amend Appendix B to part 364 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

Dated at Washington, DC, this 18th day of March, 2005.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR CHAPTER V

Authority and Issuance

■ For the reasons set out in the joint preamble, the OTS amends parts 568 and 570 of chapter V of title 12 of the Code of Federal Regulations to read as follows:

PART 568—SECURITY PROCEDURES

■ 1. Revise the part heading for part 568 to read as shown above.

■ 2. Revise the authority citation for part 568 to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, 1881–1884; 15 U.S.C. 1681s and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

■ 3. Amend § 568.5 by adding a new sentence after the final sentence to read as follows:

§ 568.5 Protection of customer information.

* * * Supplement A to Appendix B to part 570 provides interpretive guidance.

PART 570—SAFETY AND SOUNDNESS GUIDELINES AND COMPLIANCE PROCEDURES

■ 4. Revise the authority citation for part 570 to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, 1881–1884; 15 U.S.C. 1681s and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

■ 5. Revise the heading of Appendix B to part 570 to read as follows:

Appendix B to Part 570—Interagency Guidelines Establishing Information Security Standards

* * * * *

■ 6. Amend Appendix B to part 570 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

Dated: March 8, 2005.

By the Office of Thrift Supervision.

James E. Gilleran,

Director.

[FR Doc. 05–5980 Filed 3–28–05; 8:45 am]

BILLING CODE 4810–33–P; (25%); 6210–01–P; (25%); 6714–01–P; (25%); 6720–01–P (25%)

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 71

[Docket No. FAA–2004–19911; Airspace Docket No. 04–ASO–20]

Establishment of Class E Airspace; Cocoa Beach Patrick AFB, FL

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This action establishes Class E4 airspace at Cocoa Beach Patrick AFB, FL. Class E4 airspace designated as an extension to Class D airspace is required when the control tower is open to contain existing Standard Instrument Approach Procedures (SIAPs) and other Instrument Flight Rules (IFR) operations at the airport. This action establishes a Class E4 airspace extension that is 6.8 miles wide and extends 7.3 miles northeast of the airport.

EFFECTIVE DATE: 0901 UTC, July 7, 2005.

FOR FURTHER INFORMATION CONTACT: Mark D. Ward, Manager, Airspace and Operations Branch, Eastern En Route and Oceanic Service Area, Federal Aviation Administration, P.O. Box 20636, Atlanta, Georgia 30320; telephone (404) 305–5586.

SUPPLEMENTARY INFORMATION:

History

On January 21, 2005, the FAA proposed to amend part 71 of the Federal Aviation Regulations (14 CFR part 71) by establishing Class E4 airspace Cocoa Beach Patrick AFB, FL, (70 FR 3155). This action provides adequate Class E4 airspace for IFR operations at Cocoa Beach Patrick AFB. Class E airspace designations for airspace areas designated as an extension to a Class D airspace area are published in Paragraph 6004 of FAA Order 7400.9M, dated August 30, 2004, and effective September 16, 2004, which is incorporated by reference in 14 CFR 71.1. The Class E airspace designation listed in this document will be published subsequently in the Order.

Interested parties were invited to participate in this rulemaking proceeding by submitting written comments on the proposal to the FAA. No comments objecting to the proposal were received.

The Rule

This amendment to Part 71 of the Federal Aviation Regulations (14 CFR part 71) establishes Class E4 airspace and at Cocoa Beach Patrick AFB, FL.

The FAA has determined that this regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore, (1) is not a "significant regulatory action" under Executive Order 12866; (2) is not a "significant rule" under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. Since this is a routine matter that will only affect air traffic procedures and air navigation, it is certified that this rule will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

Adoption of Amendment

■ In consideration of the foregoing, the Federal Aviation Administration amends 14 CFR part 71 as follows:

Sundberg, Christopher

From: Richards, Mike
Sent: Tuesday, September 13, 2005 3:27 PM
To: Sundberg, Christopher
Subject: Amendment Language

Changes to Senate Bill 164
Tuesday, September 13, 2005

This memorandum was put together to change LRBs0205/1. Below are the changes that we would like to see made to this draft.

Pg. 1, line 4: Change to read: …Notice of unauthorized ACQUISITION…

Pg. 2, line 15: Delete the entire line

Pg. 4 lines 3-12, change to read:

"(3m) REGULATED ENTITIES EXEMPT. This section does not apply to an entity that is required by federal law or regulation to maintain security breach procedures so long as the entity provides notice in accordance with the requirements of the federal law or regulation."

In other words, rewrite and delete lines 5-7 and 10-12

Please add the following to the draft:

"An entity or its affiliates that is subject to and examined for, and in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter."

Also add:

"An entity that is governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 199 (HIPPA) shall be deemed in compliance with this chapter."

Michael D. Richards

Michael D. Richards
Office of State Senator Ted Kanavas
State Capitol, Room 10 South
Madison, WI 53707-7882
608-266-9174

Sundberg, Christopher

From: Richards, Mike
Sent: Wednesday, September 14, 2005 11:35 AM
To: Sundberg, Christopher
Subject: RE: Easy question

Tomorrow by noon if at all possible.

By the way, there may be two more changes/additions:

For the data types: please change line 16 on page 2 to read....in s.943.201 (1) (b) 4., 5., 9., 11., 12a. and 12c., 13.

There may also be a change to include in the exempt the student records from the University. I am trying to get the information on this.

From: Sundberg, Christopher
Sent: Wednesday, September 14, 2005 11:16 AM
To: Richards, Mike
Subject: Easy question

Is there a specific deadline for this? I'm just wondering if I have time to do an analysis.

Christopher Sundberg
Legislative Attorney
Legislative Reference Bureau
(608) 266-9739
christopher.sundberg@legis.state.wi.us

Sundberg, Christopher

From: Richards, Mike
Sent: Wednesday, September 14, 2005 4:06 PM
To: Sundberg, Christopher
Subject: RE: Easy question

Chris,

I have the information for you, and I think it should be final.

Here what we would like to see the final draft to reflect:

- Page 3, line 2--change the word individual to person. The senator is adamant about changing that.
- Any of the new language that you have drafted pertaining to the exempted entities, if you use the word individual change it to person. This is so that these entities are in compliance with the federal regulations.

9/14: Spoke to Mike about "person" vs. "individual." Pointed out that "individual" is used because under the draft, "personal information" only pertains to individuals, not other entities, such that an entity should not be in a position of notifying anyone other than an "individual." Mike indicated that "person" should still be substituted.

CS.

Gibson-Glass, Mary

From: Richards, Mike
Sent: Thursday, September 15, 2005 9:36 AM
To: Gibson-Glass, Mary; Sundberg, Christopher
Subject: Senate Bill 164

Mary,

Chris told me to contact you this morning if I needed anything on SB 164, since he is out this morning.

We have one change to the draft, and it should be ready for editing....

In the exemption language----

If the section reads something to the effect of ----this section does not apply to an entity which is required by federal law or regulation, **OR BY A CONTRACT THAT IS REQUIRED UNDER FEDERAL LAW.....**

We would like to add the phrase in bold to ensure that the affliliates who are also required to provide notification under federal guidlines are also covered. Thanks.

Michael D. Richards

Michael D. Richards
Office of State Senator Ted Kanavas
State Capitol, Room 10 South
Madison, WI 53707-7882
608-266-9174

conf. w/ Mike. ... a
of sub. (3m)
wants par. (a) ~~to~~ in

to apply to contracted
of the financial
institution

In: 9/14/05 4:30 pm
Due: tomorrow by noon, please
end of day

P1

0206/1

2005 – 2006 LEGISLATURE

LRBs~~0205/1~~
CTS:all:jf

RunNR

keep

SENATE SUBSTITUTE AMENDMENT ,

TO 2005 SENATE BILL 164

Redraw √+

AN ACT ***to create*** 895.507 of the statutes; **relating to:** notice regarding unauthorized acquisition of personal information. ✓

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

(3) - acquisition ✓

SECTION 1. 895.507 of the statutes is created to read:

(4) **895.507 Notice of unauthorized ~~use~~ of personal identifying information. (1)** DEFINITIONS. In this section:

(a) 1. "Entity" means a person, other than an individual, that does any of the following:

a. Conducts business in this state and maintains personal information in the ordinary course of business.

b. Stores personal information in this state.

c. Maintains for a resident of this state a depository account as defined in s. 815.18 (2) (e).

d. Lends money to a resident of this state.

2. "Entity" includes all of the following:

a. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts.

b. A city, village, town, or county.

(am) "Name" includes all of the following:

1. An individual's first name.

2. The first letter of an individual's first name combined with the individual's last name.

(b) Except as provided in par. (c), "personal information" means any of the following information if the information is accompanied by the name of the individual to whom the information pertains and is not publicly available:

1. An individual's electronic mail address.

2. Any of the information specified in s. 943.201 (1) (b) 4., 5., and 9. to 14.

(c) "Publicly available information" means any information that an entity reasonably believes is one of the following:

1. Information that is lawfully made widely available through any media.

2. Information that is lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.

(2) NOTICE REQUIRED. (a) If an entity whose principal place of business is located in this state or an entity that stores personal information in this state knows that personal information in the entity's possession has been acquired by a person

whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each individual who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the individual.

(b) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the individual.

(cm) Notwithstanding pars. (a) and (b), an entity is not required to provide notice of the acquisition of personal information in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

(3) TIMING AND MANNER OF NOTICE. (a) Subject to sub. (5), an entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 30 business days after the entity learns of the acquisition of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

(b) An entity shall provide the notice required under sub. (2) by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity

shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.

(3m) REGULATED ENTITIES EXEMPT. This section does not apply to an entity that is required by federal law or regulation to provide notice of the acquisition of personal information by a person whom the entity has not authorized to acquire the personal information or to provide notice of a similar breach of the security of personal information in the entity's possession, if all of the following apply:

(a) The entity provides notice in accordance with the requirements of the federal law or regulation.

(b) The entity provides notice within a reasonable time, not to exceed 30 days, after the entity learns of the acquisition of personal information or similar breach of the security of personal information in the entity's possession.

(4) EFFECT ON CIVIL CLAIMS. An entity that complies with this section is not liable for damages caused by the acquisition of personal information by a person whom the entity has not authorized to acquire the personal information. Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

(5) REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

(6m) LOCAL ORDINANCES OR REGULATIONS PROHIBITED. No city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

(7m) EFFECT OF FEDERAL LEGISLATION. If the joint committee on administrative rules determines that the federal government has enacted legislation that imposes notice requirements substantially identical to the requirements of this section and determines that the legislation does not preempt this section, the joint committee on administrative rules shall submit to the revisor of statutes for publication in the Wisconsin administrative register a notice of its determination. This section does not apply after publication of a notice under this subsection.

(END)

Insert 4–13:

(a) An entity that is a financial institution subject to the interagency guidance on response programs for unauthorized access to customer information and customer notice published in the Federal Register on March 29, 2005, if the entity complies with the interagency guidance.

(b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with the requirements of 45 CFR part 164.

**** Redid par. (a) per Kanavas request. See e-mail and review please. Mon

2. In compliance with the interagency guidance specified in subd. 1. or any person under contract with with that entity that is all of the following:

1. Subject

State of Wisconsin
2005 – 2006 LEGISLATURE

LRBs0206/1
CTS:all:pg

SENATE SUBSTITUTE AMENDMENT ,

TO 2005 SENATE BILL 164

AN ACT *to create* 895.507 of the statutes; **relating to:** notice regarding unauthorized acquisition of personal information.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 895.507 of the statutes is created to read:

895.507 Notice of unauthorized acquisition of personal identifying information. (1) DEFINITIONS. In this section:

(a) 1. "Entity" means a person, other than an individual, that does any of the following:

a. Conducts business in this state and maintains personal information in the ordinary course of business.

b. Stores personal information in this state.

c. Maintains for a resident of this state a depository account as defined in s. 815.18 (2) (e).

d. Lends money to a resident of this state.

2. "Entity" includes all of the following:

a. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts.

b. A city, village, town, or county.

(am) "Name" includes all of the following:

1. An individual's first name.

2. The first letter of an individual's first name combined with the individual's last name.

(b) "Personal information" means any of the information specified in s. 943.201 (1) (b) 4., 5., 9., 11., 12. a. and c., and 13. if the information is accompanied by the name of the person to whom the information pertains and is not publicly available.

(c) "Publicly available information" means any information that an entity reasonably believes is one of the following:

1. Information that is lawfully made widely available through any media.

2. Information that is lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.

(2) NOTICE REQUIRED. (a) If an entity whose principal place of business is located in this state or an entity that stores personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each person who is the subject of the personal

information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the ~~person~~ subject of the personal information.

(b) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the ~~individual~~ person. resident of this state who is the subject of the personal information

(cm) Notwithstanding pars. (a) and (b), an entity is not required to provide notice of the acquisition of personal information in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

(3) TIMING AND MANNER OF NOTICE. (a) Subject to sub. (5), an entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 30 business days after the entity learns of the acquisition of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

(b) An entity shall provide the notice required under sub. (2) by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.

(3m) REGULATED ENTITIES EXEMPT. This section does not apply to any of the following:

such an

(a) An entity that is a financial institution, or any person under contract with that entity, that is all of the following:

1. Subject to the interagency guidance on response programs for unauthorized access to customer information and customer notice as published in the federal register on March 29, 2005.

2. In compliance with the interagency guidance specified in subd. 1.

****NOTE: I redid par. (a) per Kanavas request. See e-mail and review please. MGG.

(b) An entity that is described in 45 CFR 164.104 (a), if the entity complies with the requirements of 45 CFR part 164.

(4) EFFECT ON CIVIL CLAIMS. An entity that complies with this section is not liable for damages caused by the acquisition of personal information by a person whom the entity has not authorized to acquire the personal information. Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

(5) REQUEST BY LAW ENFORCEMENT NOT TO NOTIFY. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period. Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

(6m) LOCAL ORDINANCES OR REGULATIONS PROHIBITED. No city, village, town, or county may enact or enforce an ordinance or regulation that relates to notice or disclosure of the unauthorized acquisition of personal information.

(7m) EFFECT OF FEDERAL LEGISLATION. If the joint committee on administrative rules determines that the federal government has enacted legislation that imposes notice requirements substantially identical to the requirements of this section and determines that the legislation does not preempt this section, the joint committee on administrative rules shall submit to the revisor of statutes for publication in the Wisconsin administrative register a notice of its determination. This section does not apply after publication of a notice under this subsection.

(END)

DRAFTER'S NOTE
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRBs0206/1dn
CTS:...:...
lmk

(date)

Sen. Kanavas:

Please review this draft carefully to ensure it is consistent with your intent. Please note that I have removed the word "identifying" from line 4 on page 1, in order to be consistent with the substance of the draft.

Christopher T. Sundberg
Legislative Attorney
Phone: (608) 266–9739
E–mail: christopher.sundberg@legis.state.wi.us

DRAFTER'S NOTE
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRBs0206/1dn
CTS:lmk:pg

September 15, 2005

Sen. Kanavas:

Please review this draft carefully to ensure it is consistent with your intent. Please note that I have removed the word "identifying" from line 4 on page 1, in order to be consistent with the substance of the draft.

Christopher T. Sundberg
Legislative Attorney
Phone: (608) 266–9739
E–mail: christopher.sundberg@legis.state.wi.us